REMARKS

Introduction

Claims 1-12 are pending. Claims 1, 11, and 12 are independent. Claims 1 and 7 have been amended. Claims 11 and 12 have been added.

Rejections under 35 U.S.C. § 102(e)

Claims 1-10 stand rejected under 35 U.S.C. 103(a) as unpatentable over U.S. Patent Application Publication No. 2004/0148259 (Reiners et al.) in view of U.S. Patent Application Publication No. 2004/0068559 (Shaw).

Reiners et al. describes a transaction authorization system for access to online banking accounts. The online bank account may include, for example, an electronic or virtual credit card account, an electronic or virtual debit card account, or the like. To prevent fraudulent access to the account, the user is provided with the ability to "enable" or "disable" the account. By "enabled" is meant that transactions performed using the bank account are authorized, and by "disabled" is meant that transactions performed using the bank account are unauthorized. The account holder enables or disables the account via an account status database. The account holder enables or disables their account by logging into an account administrative server, during which the account holder is authenticated by entering a correct username and password (see page 2, paragraph [0034], or FIG. 3, block 54). Alternatively, the account administrative server may require identification via a smart card, digital certificate, or via biometric data, such as a fingerprint. The account holder enables or disables an account based on a pre-selected condition, such as a specified time period or a predetermined event, such as a maximum number of attempted logins. A third party merchant, at a later date, may attempt to access the account for the purpose of a bank transaction. The transaction is authorized in a convention fashion by

checking account balance or credit lint, but in addition, the transaction may take place only if the account is "enabled."

In contrast to the system described by Reiners et al., amended claim 1 of the present application recites, *inter alia*, a method for effecting controlled access to a privileged account by the account holder on a computer system, whereby the computer system receives a login into an account with a user id and an account name; determines whether the account name is in a list of privileged account names and allowing access to the account if the account name is not in the privileged account list; determines whether the user id is in a list of user ids having permission to access privileged accounts and allowing access to the account if the user id is in the list of user ids having permission to access privileged accounts; prompts the account holder for a reason for accessing the account; records a reason for accessing the account which was entered by the user; notifies a manager of the privileged account of the login; records keystrokes in a log file while logged into the account; terminates the login; and notifies the manager of the privileged account of the login termination.

Reiners et al. does not describe prompting for a reason for accessing the account nor recording a reason for accessing the account The Examiner states that recording a reason for accessing the account can be found at Reiners et al., paragraphs [0020, 0021]. Paragraphs [0020, 0021] merely state that the system may contain an authentication facility for authenticating the identity of the bank holder via an account holder interface. The account holder interface accesses and interrogates the account status database to obtain a transaction record or statement. Nowhere is it specified or suggested that the user is prompted to enter a reason for using an account. Elsewhere in Reiners et al., as described above, the account holder is authenticated by entering a correct username and password (see page 2, paragraph [0034], or FIG. 3, block 54). Alternatively, the account administrative server may require identification via a smart card,

digital certificate, or via biometric data, such as a fingerprint. Accordingly, applicant submits that Reiners et al. does not describe, teach, or provide motivation for the invention recited by amended claim 1 of the present application.

Shaw fails to correct the deficiencies of Reiners et al. Shaw describes a method for detecting unauthorized computer system usage by monitoring a user's activities, such as keystrokes, uploading bytes, or downloading bytes. The unauthorized activity may be recorded in an activity log or may be terminated by the computer system. There is no mention anywhere in Shaw of the process of a user logging into an account, and whether this login process includes prompting for and receiving a reason for logging into the account. Accordingly, applicant submits that neither Reiners et al. nor Shaw, alone or in combination, describes, teaches, or provides motivation for the invention recited by amended claim 1 of the present application. As such, withdrawal of the rejection of claim 1 under 35 U.S.C. 103(a) based on Reiners et al. in view of Shaw is requested.

Each of claims 2-10 ultimately depend from claim 1, that has been shown to be patentable, and is likewise deemed to be patentable, for at least the reasons described above with respect to the patentability of claim 1.

Independent Claims 11 and 12 have been added. Independent Claims 11 and 12 are directed to methods for effecting controlled access to a privileged account on a computer system running a Unix-like operating system, which include the steps deemed to be patentable over the references of record for amended independent claim 1. As such, new independent claims 11 and 12 are in condition for allowance.

Thus, applicant submits that each of the claims of the present application are patentable over each of the references of record, either taken alone, or in any proposed

hypothetical combination. Accordingly, withdrawal of the rejections to the claims is respectfully requested.

Conclusion

In view of the above remarks, reconsideration and allowance of the present application is respectfully requested. No fee is believed to be due in connection with this Amendment. If, however, other fees are deemed necessary for this Amendment to be entered and considered by the Examiner, then the Commissioner is authorized to charge such fee to Deposit Account No. 50-1358. Applicant's undersigned patent agent may be reached by telephone at (973) 597-2500. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

Date: 4/9/07

Raymond G. Cappo
Patent Agent for Applicant
Registration No. 53,836

DOCKET ADMINISTRATOR
LOWENSTEIN SANDLER PC
65 Livingston Avenue
Roseland, NJ 07068